PATENT ABSTRACTS OF JAPAN

(11)Publication number : 64-074582
(43)Date of publication of application : 20.03.1989

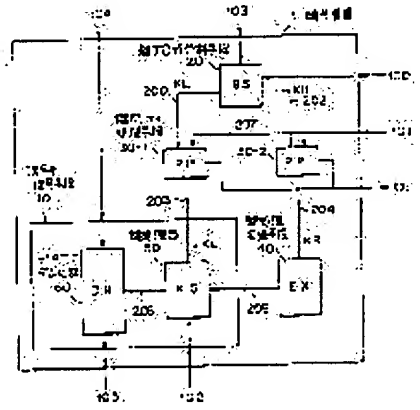
(51)Int.Cl. G09C 1/00

(21)Application number : 62-232957
(22)Date of filing : 16.09.1987

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : MIYAGUCHI SHOJI

(54) CIPHERING DEVICE

(57)Abstract:
PURPOSE: To attain a ciphering device having key length consisting of 2N bits by a ciphering/deciphering means having key length consisting of N bits by dividing an inputted 2N-bit key block into two parts, extending N bits of one divided part by a prescribed value and ciphering and deciphering the extended bits as a parameter.
CONSTITUTION: An input of 128 bits or the like is divided into two 64-bit key blocks KL, KR by a key block dividing means 20 in a ciphering/deciphering means 1 consisting of 64 bits or the like. The block KR transmitted through a key parity processing means 30-2 is extended to 96 bits or the like more than 3/2 x 64 bits by a key processing extending means 40 and the extended block KR is supplied to a key processing part 50 in a ciphering/deciphering means 10 to which the block KR transmitted through a parity processing means 30-1 is also supplied. A normal sentence consisting of 128 bits applied to a data randomizing part 60 is ciphered by 12 parameters of 16-bit length or the like outputted from the processing part 50. Since deciphering is similarly executed, the 2N-bit ciphering device can be attained by the ciphering/deciphering means having N-bit key length.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)　(11)特許出願公開

(12)公開特許公報(A)　昭64-74582

(51)Int.Cl.⁴　識別記号　庁内整理番号　(43)公開　昭和64年(1989)3月20日

G 09 C 1/00　7368-5B

審査請求　未請求　発明の数 1　(全6頁)

(54)発明の名称　暗号装置

(21)特　願　昭62-232957

(22)出　願　昭62(1987)9月16日

(72)発明者　宮口　庄司　東京都千代田区内幸町1丁目1番6号　日本電信電話株式会社内

(71)出願人　日本電信電話株式会社　東京都千代田区内幸町1丁目1番6号

(74)代理人　弁理士　草野　卓

明　細　書

1.発明の名称

暗　号　装　置

2.特許請求の範囲

(1)　入力された2Nビットの鍵ブロックを各Nビットの鍵ブロックに分割する鍵ブロック分割手段と、

その分割された鍵ブロックの一方を$\frac{3}{2}$Nビット以上の鍵ブロックに拡張する鍵処理拡張手段と、

その拡張された鍵ブロックをパラメータとして、上記分割された鍵ブロックとして入力し、入力データを暗号化復号処理する鍵長がNビットの暗号化復号手段とを具備する暗号装置。

3.発明の詳細な説明

「産業上の利用分野」

この発明は、暗号鍵をパラメータとして平文から暗号文を得、及び暗号文から平文を得る暗号装置に関するものである。

「従来の技術」

従来のこの種の暗号装置は、例えば特願昭62-37231「暗号装置」に示されている。この特許出願の第1図及び第2図を組合わせて実現される暗号装置は、暗号鍵(以降:鍵という)の長さNが64ビットである。従って、この暗号装置で得た暗号文を解読するには、鍵の全て、即ち、$2^N = 2^{64}$通りの鍵について暗号文の解読を行うことができれば、暗号文は解読できる。この様な、鍵の2^{64}回のしらみつぶし検査は、現在のコンピュータ技術では不可能であるが、コンピュータの計算能力は年々向上しており、将来は可能となろう。このため、鍵の長さを64ビット以上に長くすることが必要であり、例えば鍵の長さNが128ビットの暗号装置が必要になると考えられる。

「問題点を解決するための手段」

この発明によれば鍵の長さNの暗号化復号手段に、小規模な鍵ブロック分割手段と鍵処理拡張手段とパリティ処理手段とを追加することにより、鍵の長さNの暗号装置と比較して極めて安全な、鍵の長さ2Nの暗号装置を実現する。

この発明による暗号装置は、鍵の長さがNビッ

トの暗号化復号手段に、鍵ブロック分割手段や鍵処理拡張手段等を追加することにより実現される。

この発明による暗号装置は、鍵ブロックの長さが２ＮビットとＮビットの２種類が選択でき、選択された鍵ブロックを使って、ｍビット長の平文ブロックをｍビット長の暗号文に暗号化し、及びｍビット長の暗号文ブロックをｍビット長の平文に復号する。更に、鍵パリティ処理手段をその構成要素とする場合は、鍵ブロックの中のパリティビットの有無を指定して、ｍビット長の平文ブロックを暗号化し及びｍビット長の暗号文ブロックを復号する。

この発明の従来と異なる点は鍵長がＮビットの暗号化復号手段を用いて、鍵長が２Ｎビットの暗号装置が実現できる。この暗号装置は、鍵ブロックの長さが２Ｎビットの暗号と、鍵の長さがＮビットの暗号とが選択できる。

「実施例１」

第１図はこの発明に基づく暗号装置１の一実施例のブロック図であり、Ｎ＝６４、平文ブロックや暗号文ブロック長ｍは、ｍ＝６４の例である。

暗号装置１は鍵長がＮビットの暗号化復号手段１０と、鍵ブロック分割手段（ＢＳ）２０と、鍵パリティ処理手段（ＰＰ）３０－１及び３０－２と、鍵処理拡張手段（ＥＸ）４０とよりなり、鍵処理部（ＫＳ）５０とデータランダム化部（ＤＲ）６０とにより暗号化復号手段１０が構成される。

鍵ブロック長指定入力部100は鍵ブロック長を２Ｎビット（128ビット）とするか、またはＮビット（６４ビット）とするかを指定する。

パリティビット有無指定入力部101は鍵ブロックの中にパリティビットが有るか、または無いかを指定する。

鍵ブロックの中にパリティビットを指定する場合は、鍵ブロックのビット位置番号８×ｉ，１≦ｉのビットとする。ここで、ブロックの中のビット位置はそのブロックの最左端ビット（ＭＳＢ）から右側へ、１，２，…と数える。

102は暗号装置の暗号化動作、または復号動作を指定する暗号化復号指定入力部であり、103は鍵ブロック入力部であり、104はデータ入力部であり、105はデータ出力部である。信号線は、200番台の番号で図中に示す。

次に暗号装置１の各構成要素についてその機能を説明する。

鍵長がＮビットの暗号化復号手段１０

長さがＮビットの鍵ブロックを鍵パリティ処理手段３０－１から入力し、暗号化復号指定入力部102で暗号化を指定した場合はデータ入力部104からのｍビット（６４ビット）の平文をデータ出力部105からｍビット（６４ビット）の暗号文として出力し、暗号化復号指定入力部102で復号を指定した場合はデータ入力部104からのｍビット（６４ビット）の暗号文をデータ出力部105からｍビット（６４ビット）の平文として出力する「鍵長がＮビットのブロック暗号化復号手段」である。但し、鍵処理拡張手段４０からは何も入力しない、即ち、０を入力する。

鍵ブロック分割手段２０

鍵ブロック長指定入力部100により鍵ブロックが128ビットと指定された場合は、鍵ブロック入力部103から入力する128ビット長の鍵ブロックを６４ビットずつ２分割する。その左半分（以降ＫＬと呼ぶ）を信号線200を介して鍵パリティ処理手段３０－１へ、その右半分（以降ＫＲと呼ぶ）を、信号線202を介して鍵パリティ処理手段３０－２へそれぞれ伝える。鍵ブロックが６４ビットと指定された場合は、この６４ビット長の鍵ブロック（以降ＫＬと呼ぶ）をそのまま信号線200を介して鍵パリティ処理手段３０－１へ伝え、信号線202へは０を出力する。

鍵パリティ処理手段３０－１と３０－２

第２図により説明する。鍵パリティ処理手段30－１及び３０－２にそれぞれ入力した６４ビットデータは、８ビットずつ８分割され部分３１を通過する。このとき、８ビット長データ毎にその奇数パリティを検査するパリティ検査回路３２でパリティ検査が行われ、パリティ検査結果が部分34に伝えられ、パリティビット有無指定入力部101で鍵ブロックの中にパリティ有りを指定している

場合は、パリティ検査結果が出力部106により暗号装置の外部に伝えられ、パリティビット有無指定入力部101で鍵ブロックの中のパリティ無しを指定している場合は、パリティ検査結果は暗号装置の外部に伝えられない。部分31通過後の各データは、パリティビット有無指定入力部101(207)で鍵ブロックにパリティ有りを指定している場合は、第3図に示す零設定制御部33でパリティビットが零に変換される。パリティビット無しを指定している場合は、なんら変更を受けずそのまま通過する。

鍵処理拡張手段（ＥＸ）４０

第４図により説明する。入力した６４ビット長のデータＫＲの左半分をＫＲ０、右半分をＫＲ１で表わす。Ｕ０は排他的論理和回路４１によりＫＲ０とＫＲ１のビット対応の排他的論理和演算を行い、Ｕ０，Ｕ１，Ｕ２を（但し、Ｕ０＝KR0⊕ＫＲ１，Ｕ１＝ＫＲ０，Ｕ２＝ＫＲ１，等号＝は右辺を左辺へ代入）、信号線205へ出力する。

鍵処理部（ＫＳ）５０

第５図により説明する。信号線205から入力した各３２ビット長のデータＵ０，Ｕ１，Ｕ２は、部分５１内で分岐し、Ｕ０はデータのかき混ぜ処理を行う拡散処理段５４の１段目と４段目の回路５２へ、Ｕ１は拡散処理段５４の２段目と５段目の回路５２へ、Ｕ２は拡散処理段５４の３段目と６段目の回路５２へ入力する。ここで、回路５２は、３２ビット巾のビット対応の排他的論理和回路である。信号線203から入力した６４ビット長のデータＫＬは、分割回路５３で３２ビットずつの左データ及び右データに分割されて、複数の拡散処理段５４の縦続配列の１段目（初段）に入力される。各拡散処理段５４では右データは、そのまま次段の左データとして出力すると共に、回路５２に供給される。３２ビット巾のビット対応の排他的論理和回路５５は、前段の左データと回路５２の出力とを入力してこれらを排他的論理和演算する。データ拡散手段５６は、左データ(α)と回路５５の演算結果(β)とを入力してこれらデータを混ぜ合わせるデータ拡散処理を行い、その出力（$f_k(\alpha, \beta)$）を右データとして次段の拡散処理段５４へ出力する。回路５５は、初段の拡散処理段では適当な定数Ｄ０と回路５２の出力を入力して、その他の拡散処理段では前段の左データと回路５２の出力とを入力する。各拡散処理段５４のデータ拡散手段５６は、パラメータP_0，P_1，…，P_{11}を出力する。

パラメータの順序変更部５７は暗号化復号指定入力部102により暗号化を指定した場合のパラメータの出力順序は、P_4，P_5，P_6，P_7，P_0，P_1，P_2，P_3，P_8，P_9，P_{10}，P_{11}であり、暗号化復号指定入力部102により復号を指定した場合のパラメータの出力順序は、P_8，P_9，P_{10}，P_{11}，P_3，P_2，P_1，P_0，P_4，P_5，P_6，P_7である。鍵処理部５０から部分51を除いた部分が、特願昭62－37231の第２図の鍵処理部のブロック図に相当する部分、但し、回路５２は回路５１を追加するための追加改造部分である。

データランダム化部（ＤＲ）６０

第６図により説明する。信号線206から入力されるパラメータについては、１番目から４番目に入力されたパラメータは回路６１へ供給され、５番目～８番目に入力されたパラメータは、それぞれデータ拡散手段６４－１～６４－４に供給され、９番目から１２番目に入力されたパラメータは回路６７へ供給される。データ入力部104から６４ビットの入力データ（平文）が入力され、信号線206をへて供給される６４ビットのパラメータP_4，P_5，P_6，P_7と排他的論理和回路６１により排他的論理和演算され、その出力の左半分データと、右半分データが排他的論理和回路６２で排他的論理和演算され、次にその出力はデータのかき混ぜ処理を行うデータ拡散手段６４－１と、排他的論理和回路６５－１との組合わせによりデータのかき混ぜが行われ、以下同様にして、データ拡散手段６４－２と回路６５－２によるデータかき混ぜ、データ拡散手段６４－３と回路６５－３によるデータかき混ぜ、データ拡散手段６４－４と回路64－４によるデータかき混ぜの処理を受け、排他的論理和回路６６で右半分データと左半分データの

排他的論理和演算を、排他的論理和回路６７で、信号線206をへて供給される６４ビットのパラメータ P_8，P_9，P_{10}，P_{11} と排他的論理和演算され、その６４ビットの出力がデータランダム化部６０の出力（暗号文）となりデータ出力部105へ出力される。入力データとして暗号文を入力した場合は、以上述べたパラメータデータは、回路６１には、P_8，P_9，P_{10}，P_{11}を、データ拡散手段６４－１，６４－２，６４－３，６４－４には、P_3，P_2，P_0 P_1を、回路６７にはP_4，P_5，P_6，P_7を入力すると、暗号文が復号された平文が105から出力される。データランダム化部６０は、特願昭62－37231の第１図の暗号処理部のブロック図に相当する。

暗号装置の動作

最初に鍵ブロック長指定入力部100で、鍵ブロック長を128ビットとするか６４ビットとするかを指定し、パリティビット有無指定入力部101で鍵ブロックのパリティビット有無を指定し、暗号化復号指定入力部102で暗号化を行うか復号を行うかを指定する。鍵ブロックを鍵ブロック入力部103から入力し、暗号化指定の場合はデータ入力部104から平文を、復号指定の場合はデータ入力部104から暗号文を入力する。鍵ブロックが128ビット指定の場合は、鍵ブロックが鍵ブロック分割手段２０で２分され、その左半分（ＫＬ）は信号線200をへて鍵パリティ処理手段３０－１へ。その右半分（ＫＲ）は信号線202をへて鍵パリティ処理手段３０－２へ伝えられる。鍵ブロックの長さ６４ビットを指定した場合は、入力した鍵ブロック（ＫＬ）は信号線200をへて鍵パリティ処理手段３０－１へ伝えられ、信号線202へは０を出力する。信号線200上のブロック値をＫＬ、信号線202上のブロック値をＫＲで表わす。鍵ブロックのパリティ無しを指定した場合は、ＫＬは鍵パリティ処理手段３０－１を、ＫＲは鍵パリティ処理手段３０－２をそのまま通過し、それぞれ信号線203または204をへて鍵処理部５０または鍵処理拡張手段４０へ伝えられる。鍵ブロックのパリティ有りを指定した場合は、ＫＬとＫＲともそれらの全パリティビットが０に設定され、信号線203または204をへて鍵処理部５０または鍵処理拡張手段４０へ伝えられる。鍵ブロックのパリティエラーの有り無しの検出結果は、出力部106をへて暗号装置の外部に伝えられる。鍵処理拡張手段４０に入力したＫＲは、鍵の拡張処理を受け96ビット長データとして信号線205をへて鍵処理部５０へ伝えられる。信号線203をへて鍵処理部50に入力したデータ（ＫＬ）は、信号線205から入力された９６ビット長データと一定の処理を受ける。鍵処理部５０は、暗号化復号指定入力部102の暗号化または復号の指定に従い、各１６ビット長の１２個のパラメータPi（$1 \leq i \leq 16$）を信号線206から一定順序で出力する。データランダム化部６０はデータ入力部104からの入力データ（平文または暗号文）を、信号線206からのパラメータを受け入れて一定の処理を行い、データ出力部105から出力データ（暗号文または平文）を出力する。

以上述べた暗号装置の動作を、数式を用いて再度説明する。

ブロックＢ１，Ｂ２，…をこの順序にならべてできるブロック、即ち、Ｂ１，Ｂ２，…の連結を、（Ｂ１，Ｂ２，…）で表わす。⊕は、ブロック間のビット対応の排他的論理和演算を表わす。例えば、Ｂ１＝00001111，Ｂ２＝00111100 のとき、Ｂ１⊕Ｂ２＝00110011である。等号＝は、右辺を左辺に代入することを表わす。

（鍵ブロック分割手段２０の処理）

ＫＬ，ＫＲは６４ビット長ブロックを表わす変数とする。鍵ブロック長が128ビットを指定した場合は、入力した鍵を６４ビットずつ２分し、KL＝鍵の左半分、ＫＲ＝鍵の右半分とする。鍵ブロック長＝６４ビットを指定した場合は、ＫＬ＝入力した鍵、ＫＲ＝０とする。

（鍵パリティ処理手段３０－１と３０－２の処理）

変数ＰＡＴを６４ビット長ブロックとし、その値は、そのビット位置の８，１６，２４，３２，４０，４８，５６，６４は０、その他のビット位置は全て１とする。即ち、

ＰＡＴ＝fefefefefefefefe（１６進数表現）

とする。次に、入力した鍵の中のパリティビット有りを指定した場合に限り、KL＝KL⊕PAT，KR＝KR⊕PATとする。

（鍵処理拡張手段40の処理）

KRを、2分割し、KR0，KR1で表わす。即ち、KR＝（KR0，KR1）とする。次に、32ビット長のブロックU0，U1，U2を次式で定める。

U0＝KR0⊕KR1

U1＝KR0

U2＝KR1

（鍵処理部50の処理）

32ビット長のブロックWi，i＝1，2，3，4，5，6を次式で表わす。

$W_0 = U0$

$W_1 = U1$

$W_2 = U2$

$W_3 = U0$

$W_4 = U1$

$W_5 = U2$

する。

暗号化を指定した場合は、Piは次の順序で信号線206から出力する。

P_4，P_5，P_6，P_7，

P_8，P_1，P_2，P_3，

P_{12}，P_9，P_{10}，P_{11}

復号を指定した場合は、Piは次の順序で信号線206から出力する。

P_{12}，P_9，P_{10}，P_{11}，

P_3，P_2，P_1，P_0，

P_4，P_5，P_6，P_7

（データランダム化部60）

（暗号化指定の場合）

平文ブロックの左右それぞれ4バイトのブロックをL_0，R_0として、まず

$(L_0, R_0) = (L_0, R_0) \oplus (P_4, P_5, P_6, P_7)$

$(L_0, R_0) = (L_0, R_0) \oplus (\phi, L_0)$

続いて、r＝1～4について、RrとLrを逐次計算する。

$R_r = L_{r-1} \oplus f(R_{r-1}, P_{r-1})$

Ar，Br，Drは、32ビット長ブロックを表わす変数とする。ϕは、全ビットが0の32ビット長ブロックを表わす。KLを2分割し、左半分をA_0と右半分B_0とする、即ち、KL＝（A_0，B_0）とする。

最初に、$D_0 = \phi$、

r＝1～6について、Pi（i＝0～11）を定める。

$D_r = A_{r-1}$

$A_r = B_{r-1}$

$B_r = f_k(A_{r-1}, B_{r-1} \oplus D_{r-1} \oplus W_{r-1})$

$P_{2(r-1)} = B_{r1}$

$P_{2(r-1)+1} = B_{rr}$

ここで、B_{r1}はB_rの左半分、B_{rr}はB_rの右半分を表わし、B_r＝（B_{r1}，B_{rr}）である。関数$f_k(\alpha, \beta)$は、32ビット長ブロックのαとβを入力してその各ビットをかき混ぜる処理（データ拡散）を行い、その結果を32ビット長ブロックとして出力する関数であり、例えば、特願昭62－37231の第7図に示されるデータ拡散手段を使って実現

$L_r = R_{r-1}$

次に、R_4，L_4に対して

$(R_4, L_4) = (R_4, L_4) \oplus (\phi, R_4)$

$(R_4, L_4) = (R_4, L_4) \oplus (P_8, P_9, P_{10}, P_{11})$

暗号文ブロックは（R_4，L_4）で得られる。

ここで、関数fは（α，β）は、32ビット長ブロックのαと16ビット長のブロックβを入力してその各ビットをかき混ぜる処理（データ拡散）を行い、その結果を32ビット長ブロックとして出力する関数であり、例えば、特願昭62－37231の第5図に示されるデータ拡散手段を使って実現する。

（復号指定の場合）

暗号文ブロックの左右それぞれ4バイトのブロックをR_4，L_4として、まず、

$(R_4, L_4) = (R_4, L_4) \oplus (P_8, P_9, P_{10}, P_{11})$

$(R_4, L_4) = (R_4, L_4) \oplus (\phi, R_4)$

続いて、r＝4～1について、L_{r-1}とR_{r-1}を逐次計算する。

$L_{r-1} = R_r \oplus f(L_r, P_{r-1})$

$R_{r-1} = L_r$

最後に、L_0, R_0に対して

$(L_0, R_0) = (L_0, R_0) \oplus (\phi, L_0)$

$(L_0, R_0) = (L_0, R_0) \oplus (P_4, P_3, P_2, P_1)$

平文ブロックは、(L_0, R_0)で得られる。

「実施例２」

この発明による暗号装置の他の実施例は、実施例１から、鍵パリティ処理手段３０－１と３０－２、及び入力部101と出力部106を省いたものである。信号線200は信号線203に接続し、信号線202は信号線204へ接続する。実施例２の動作は、実施例１の動作で鍵パリティ処理手段３０－１と３０－２の動作を省いたものに等しい。

「実施例３」

この発明による暗号装置の更に他の実施例は、実施例１から、鍵ブロック分割手段２０、鍵パリティ処理手段３０－２と鍵処理拡張手段４０を省いたものである。ここで、入力部103は、信号線203へ接続する。信号線205へは、０を、即ち、U０＝０，U１＝０，U３＝０を入力する。実施例３の動作は、実施例１の動作で、鍵ブロック長＝６４ビットを指定したときの動作に等しい。

「発明の効果」

以上述べたように構成されているから、鍵長がＮビットの暗号化復号手段から、鍵長が２Ｎビットの暗号装置が容易に実現できる。

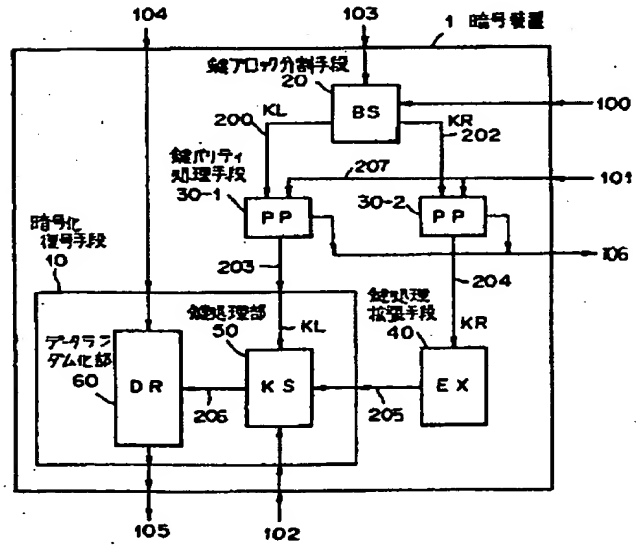
4.図面の簡単な説明

第１図はこの発明の一実施例を示すブロック図、第２図は鍵パリティ処理手段を示すブロック図、第３図は零設定制御部を示すブロック図、第４図は鍵処理拡張手段を示すブロック図、第５図は鍵処理部を示すブロック図、第６図はデータランダム化部を示すブロック図である。

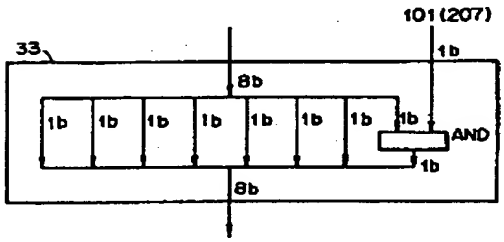
特許出願人　日本電信電話株式会社

代理人　草野　卓

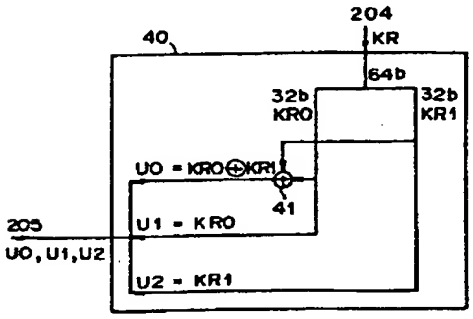
第１図



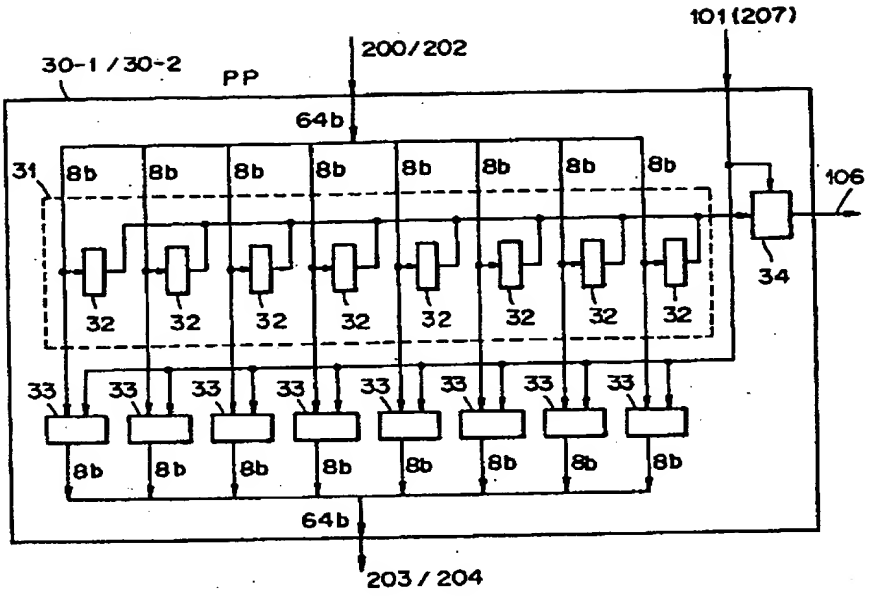
第３図



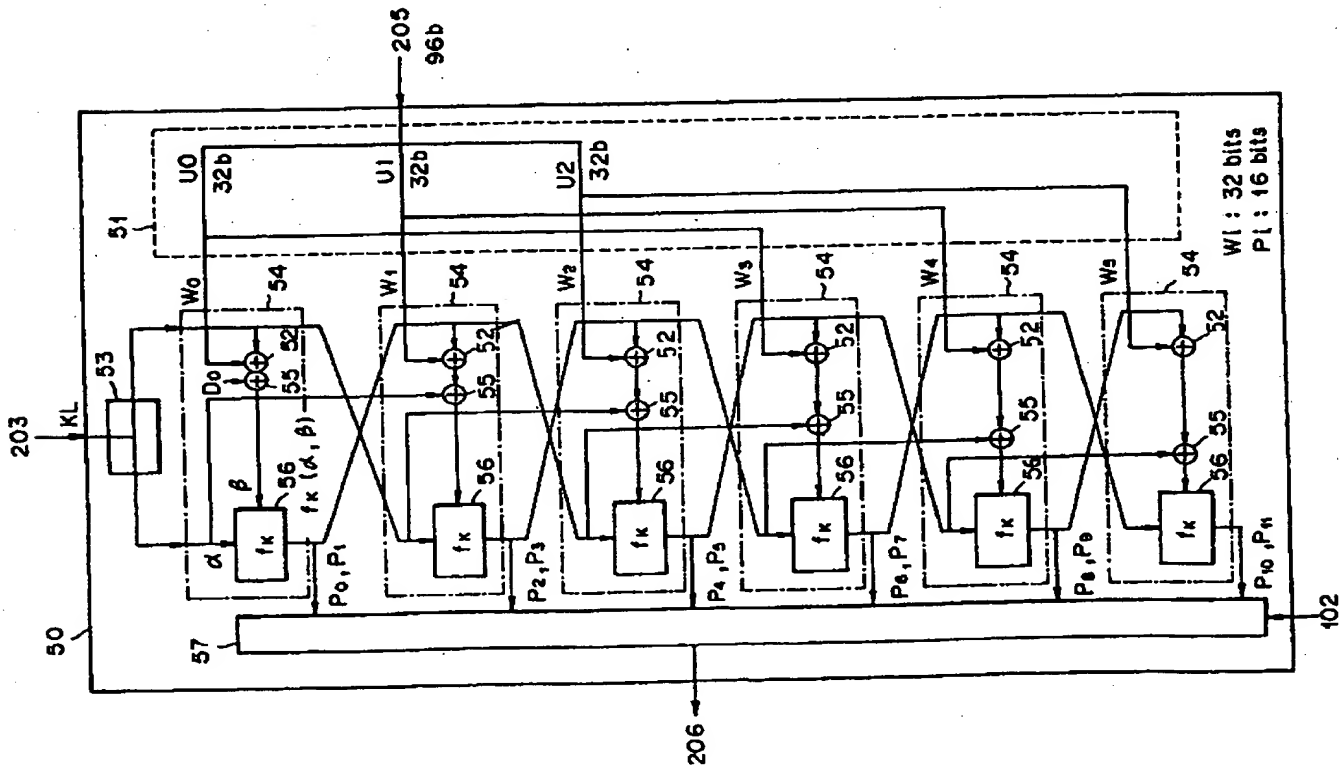
第４図

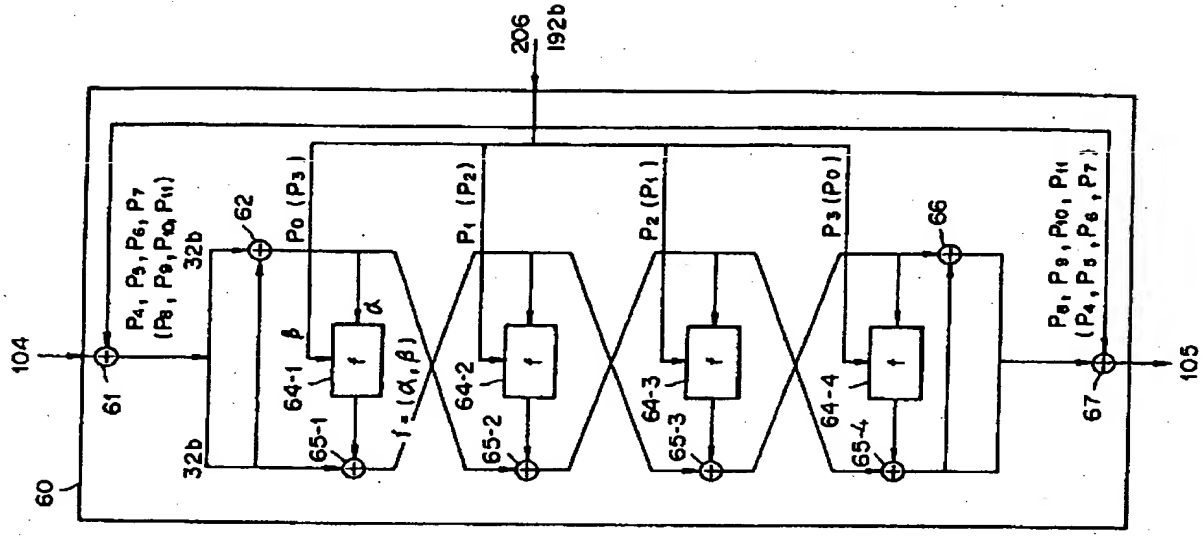


第２図


101(207)
200/202
30-1/30-2
PP
64b
31
8b
106
34
32
33
64b
203/204

第５図


205
96b
U0
U1
U2
32b
51
W0
W1
W2
W3
W4
W5
54
52
53
KL
203
55
56
Do
β
α
fK (α, β)
fK
P0, P1
P2, P3
P4, P5
P6, P7
P8, P9
P10, P11
W1 : 32 bits
P1 : 16 bits
50
57
102
206


206
192b
104
61
60
62
32b
32b
64-1
65-1
64-2
65-2
64-3
65-3
64-4
65-4
66
67
105
f
α
β
f=(α,β)

第6図